JOSEPH W. PRICE
ALBIN H. GESS
FRANKLIN D. UBELL
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE

PRICE, GESS & UBELL
ATTORNEYS AT LAW

2100 S.E. MAIN STREET, SUITE 250

IRVINE, CALIFORNIA 92614-6238

A PROFESSIONAL CORPORATION
TELEPHONE: (949) 261-8433
FACSIMILE: (949) 261-9072
FACSIMILE: (949) 261-1726

e-mail: pgu@pgulaw.com

DRAWINGS - FOURTEEN (14) SHEETS

Applicant(s):	Makoto Tatebayashi et al.
Title:	ENCRYPTION METHOD, ENCRYPTION APPARATUS, DECRYPTION METHOD, AND DECRYPTION APPARATUS
Attorney's Docket No.:	NAK1-BM08

"EXPRESS MAIL" MAILING LABEL NO. EL230379070US

DATE OF DEPOSIT: August 15, 2000

FIG.1

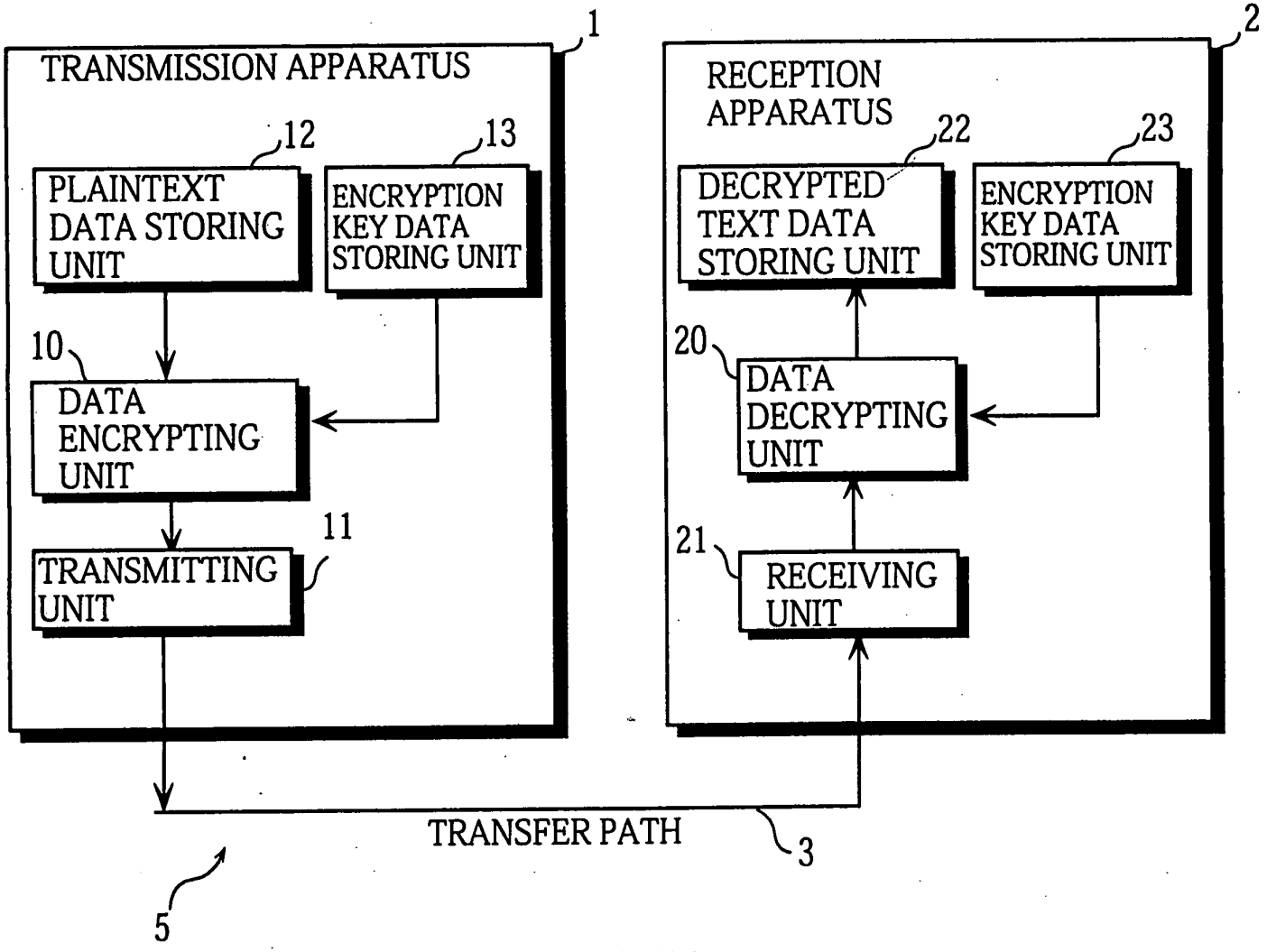

FIG.2

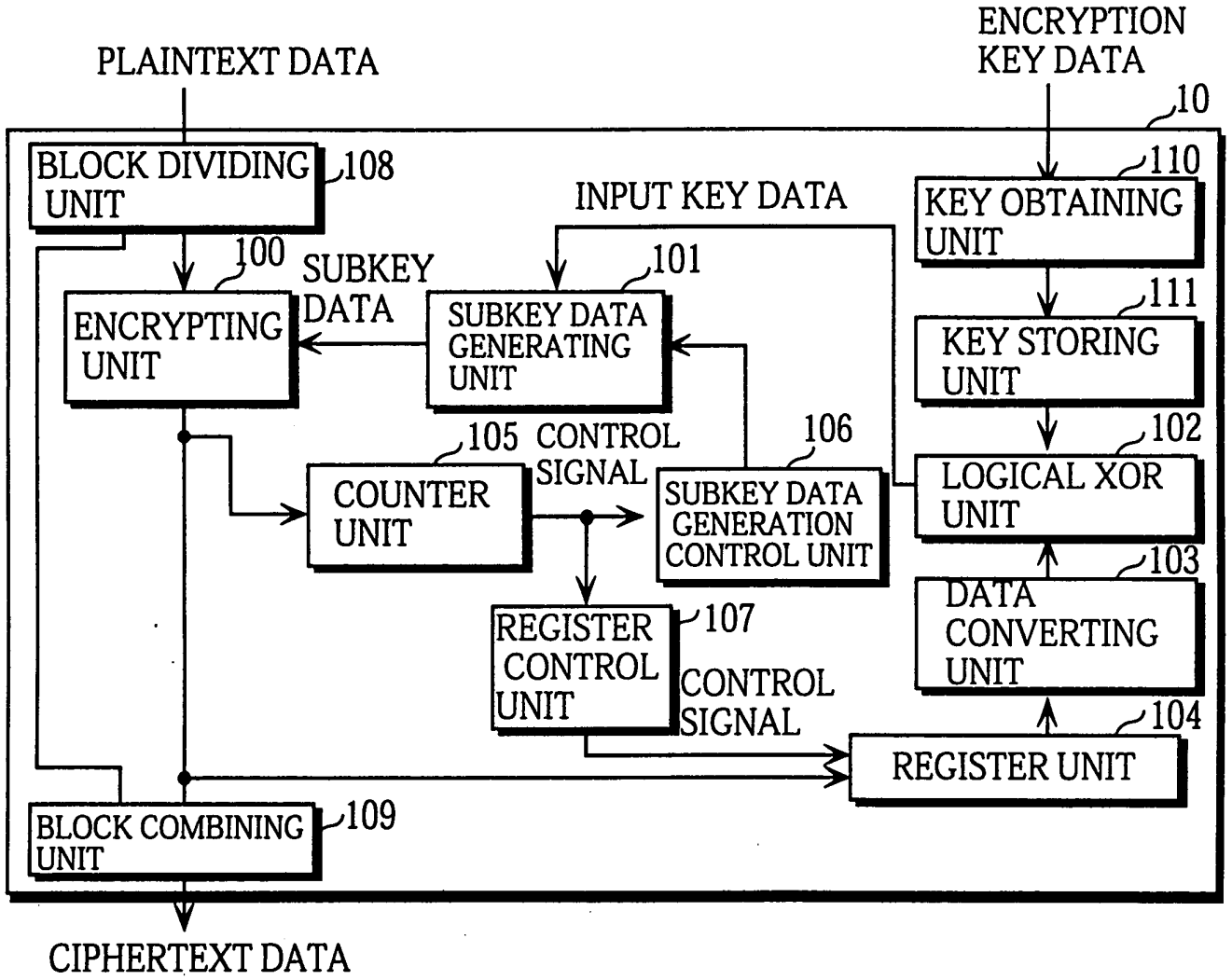

FIG.3

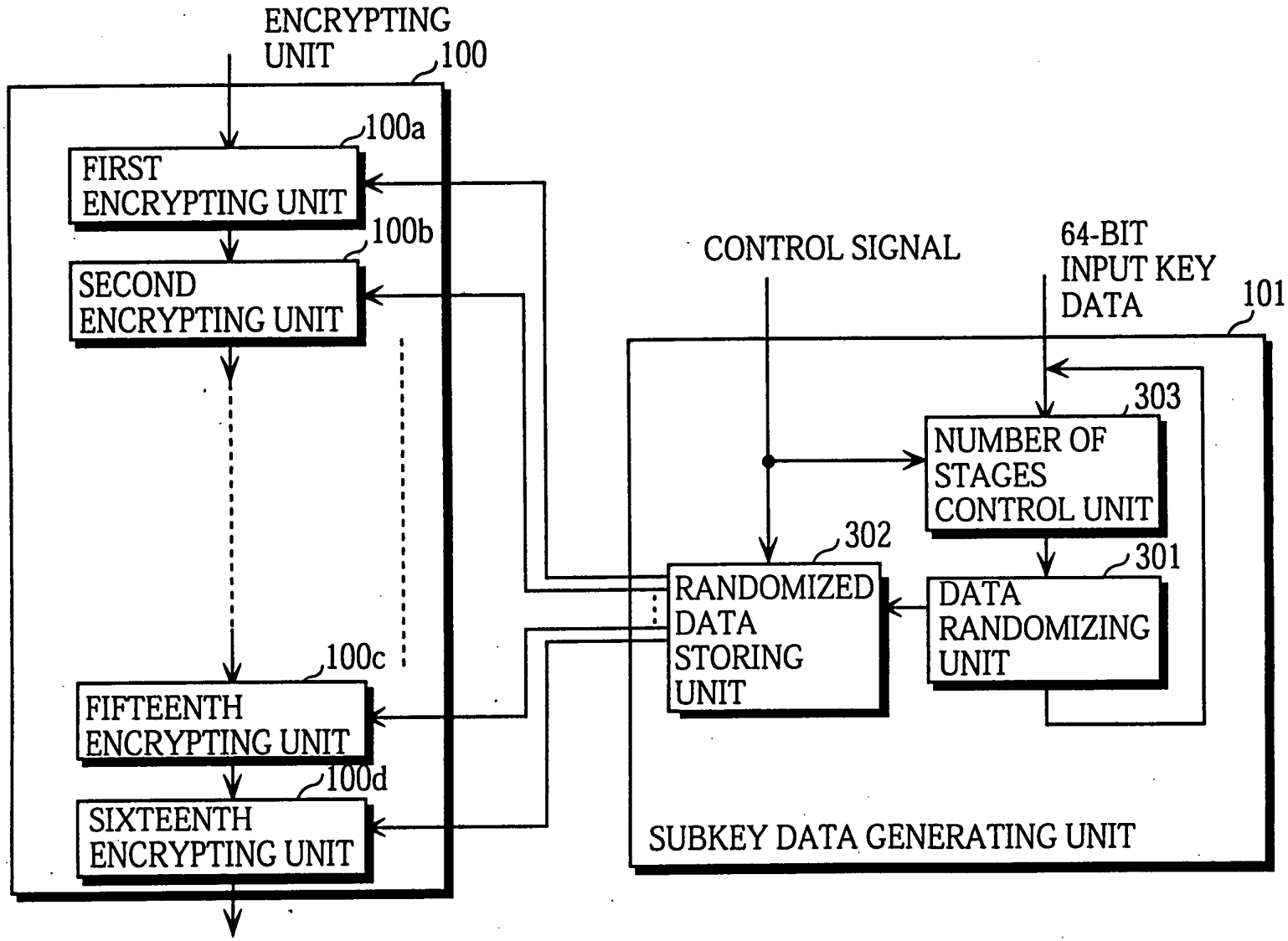

FIG. 4

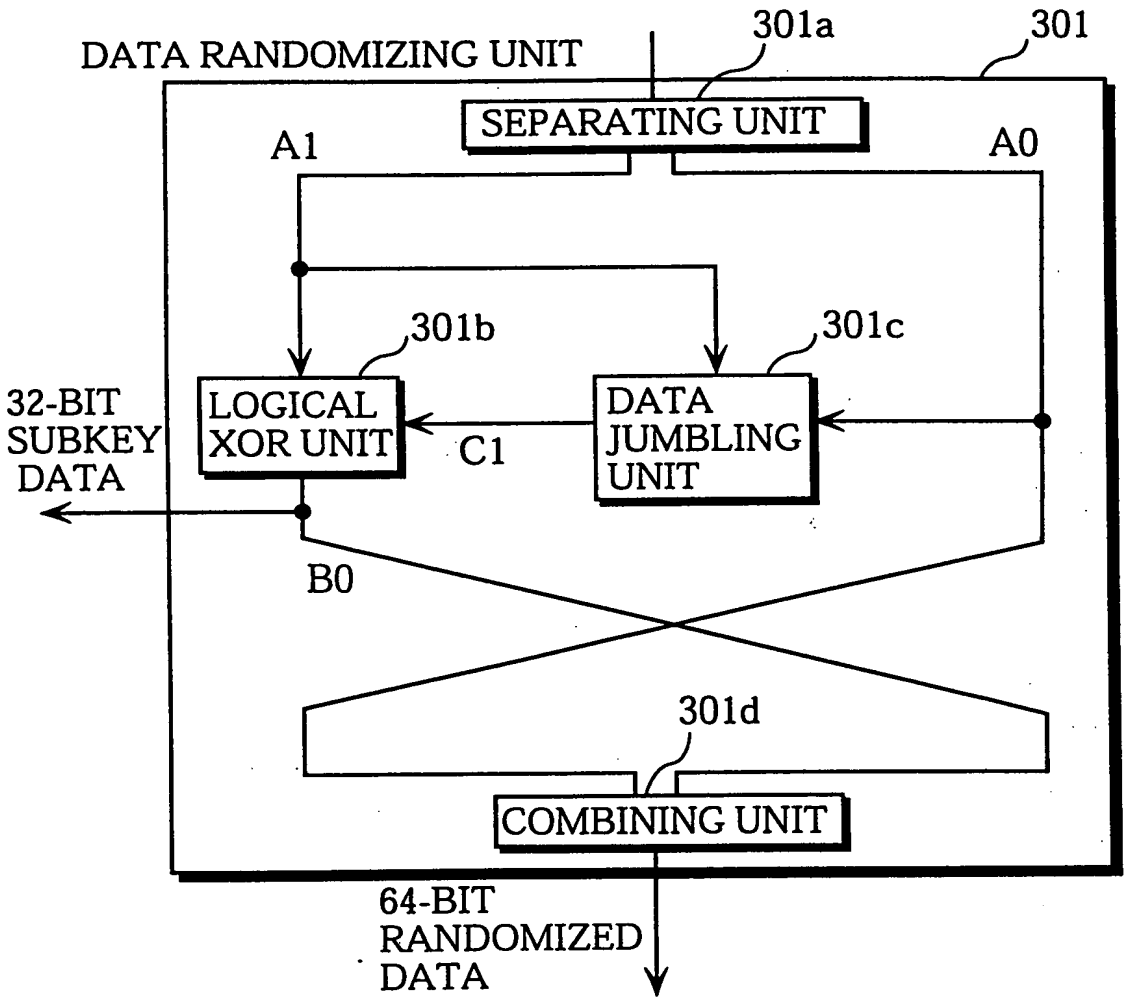
DATA RANDOMIZING UNIT
301a
301
SEPARATING UNIT
A1
A0
301b
301c
32-BIT
SUBKEY
DATA
LOGICAL
XOR UNIT
C1
DATA
JUMBLING
UNIT
B0
301d
COMBINING UNIT
64-BIT
RANDOMIZED
DATA

FIG. 5A

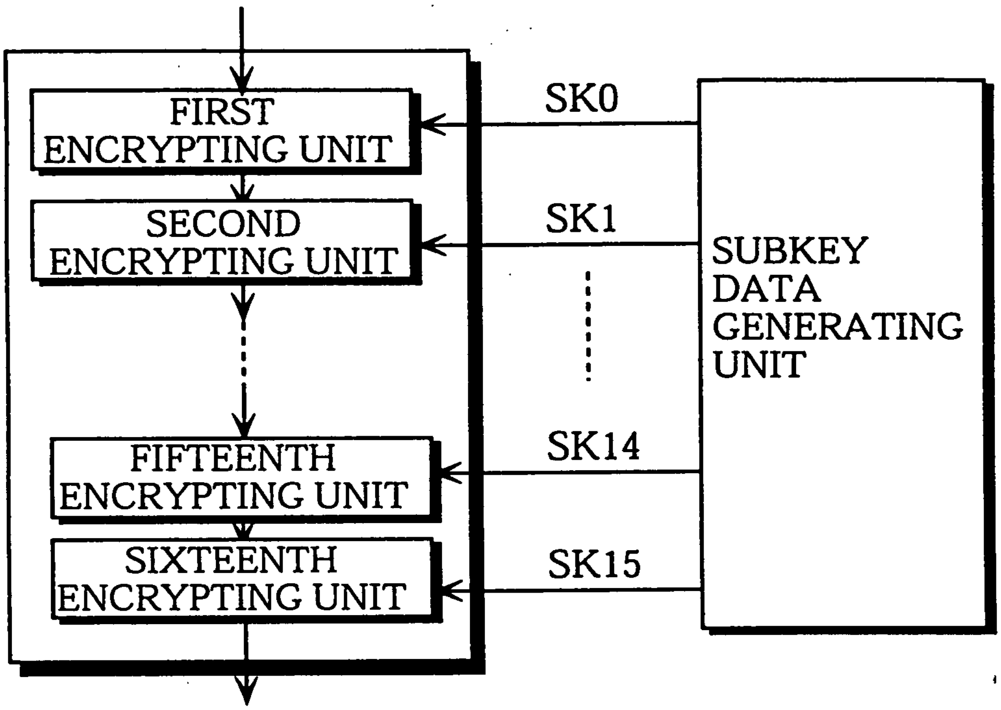

FIG. 5B

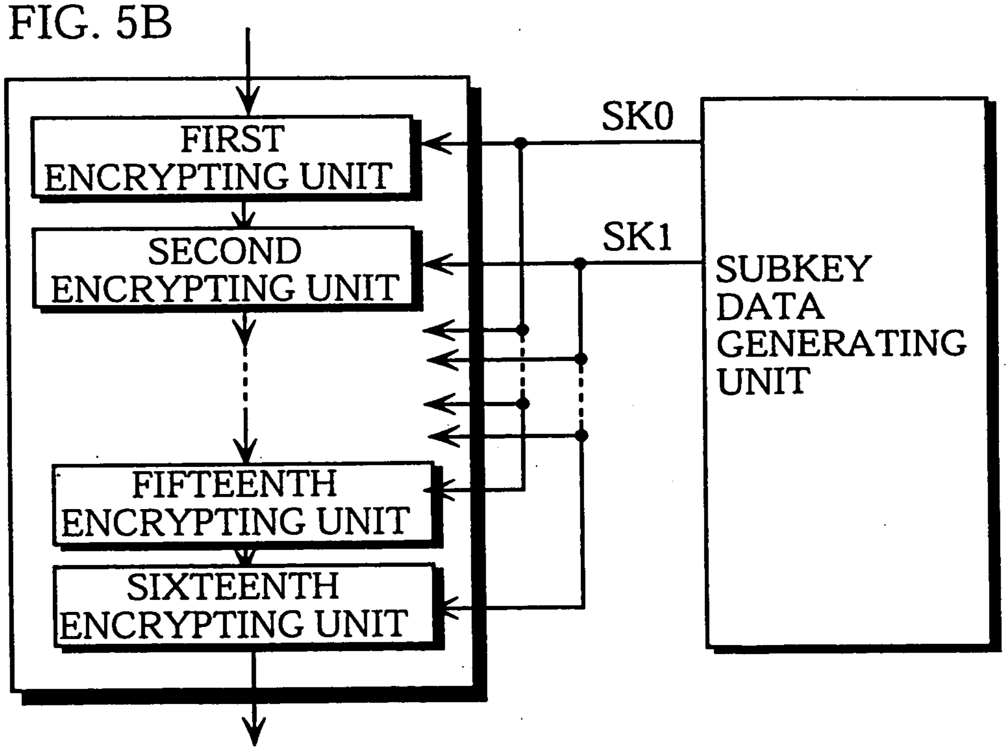

FIG.6

COUNT VALUE	INPUT KEY DATA	SUBKEY DATA GENERATION TYPE
0	EK(+) f(IV)	A
1	EK(+) f(C_0)	B
2	EK(+) f(C_1)	B
⋮	⋮	⋮
$2^{10}-1$	EK(+) f($C_{2^{10}-2}$)	B
0	EK(+) f(IV)	A
1	EK(+) f(C_0)	B
2	EK(+) f(C_1)	B
⋮	⋮	⋮
$2^{10}-1$	EK(+) f($C_{2^{10}-2}$)	B
0	EK(+) f(IV)	A
⋮	⋮	⋮

FIG.7

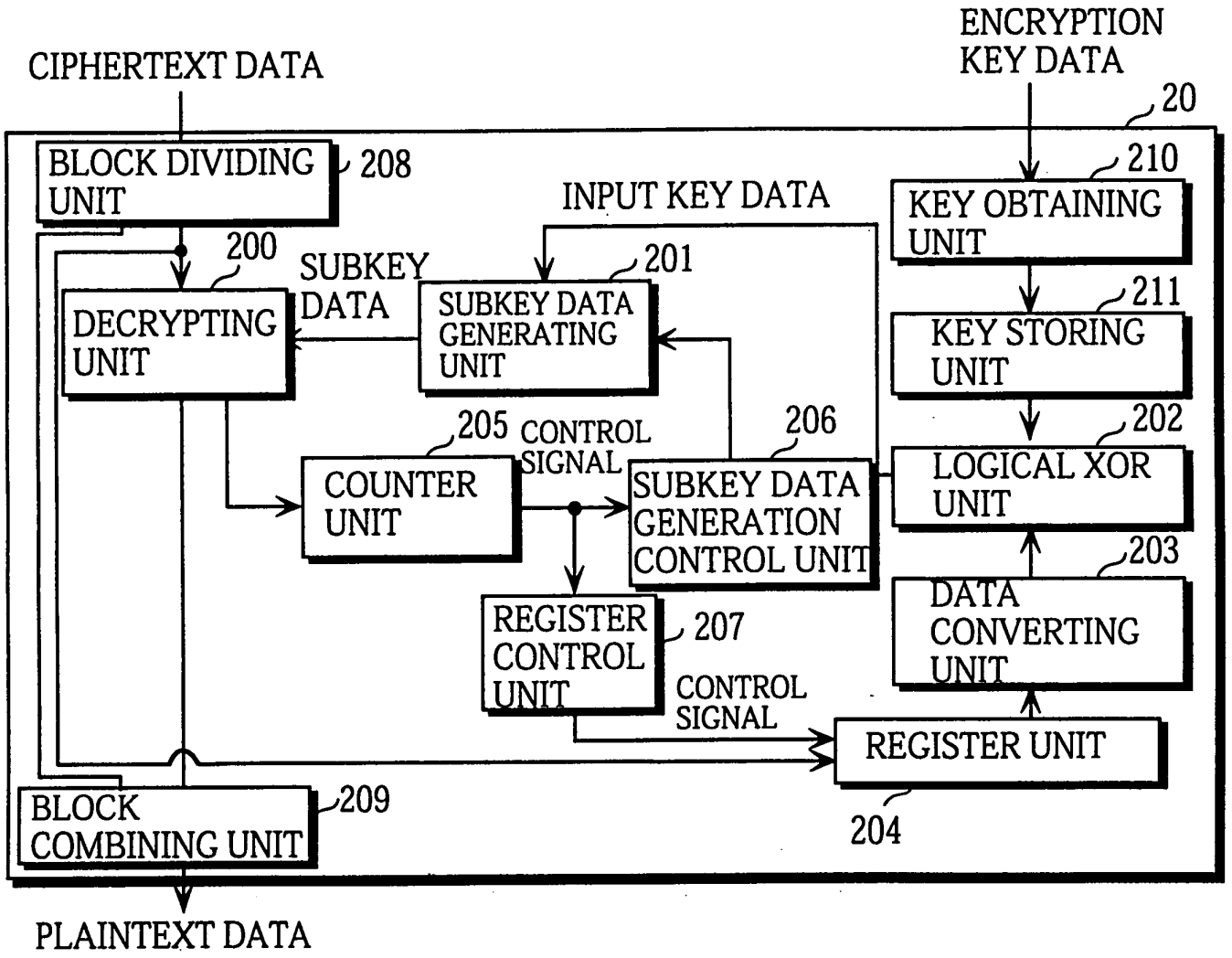

FIG. 8

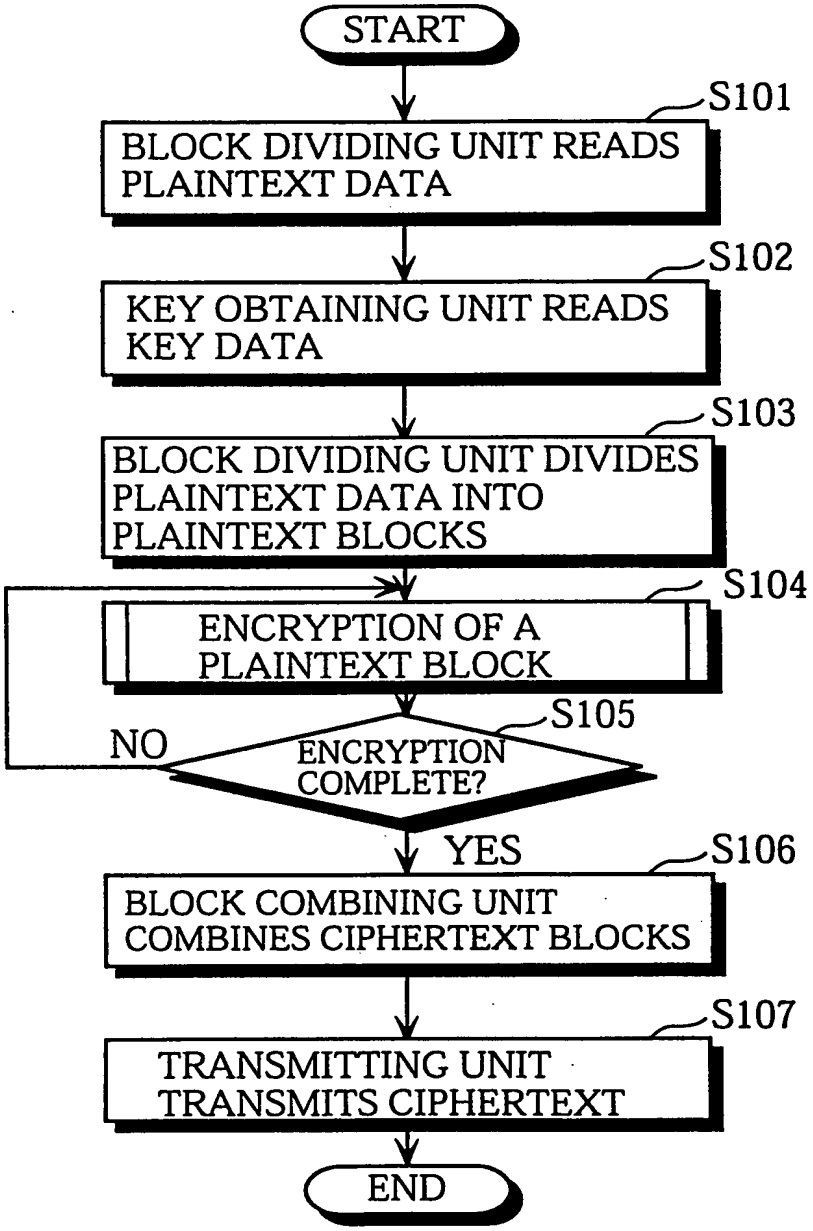

FIG.9

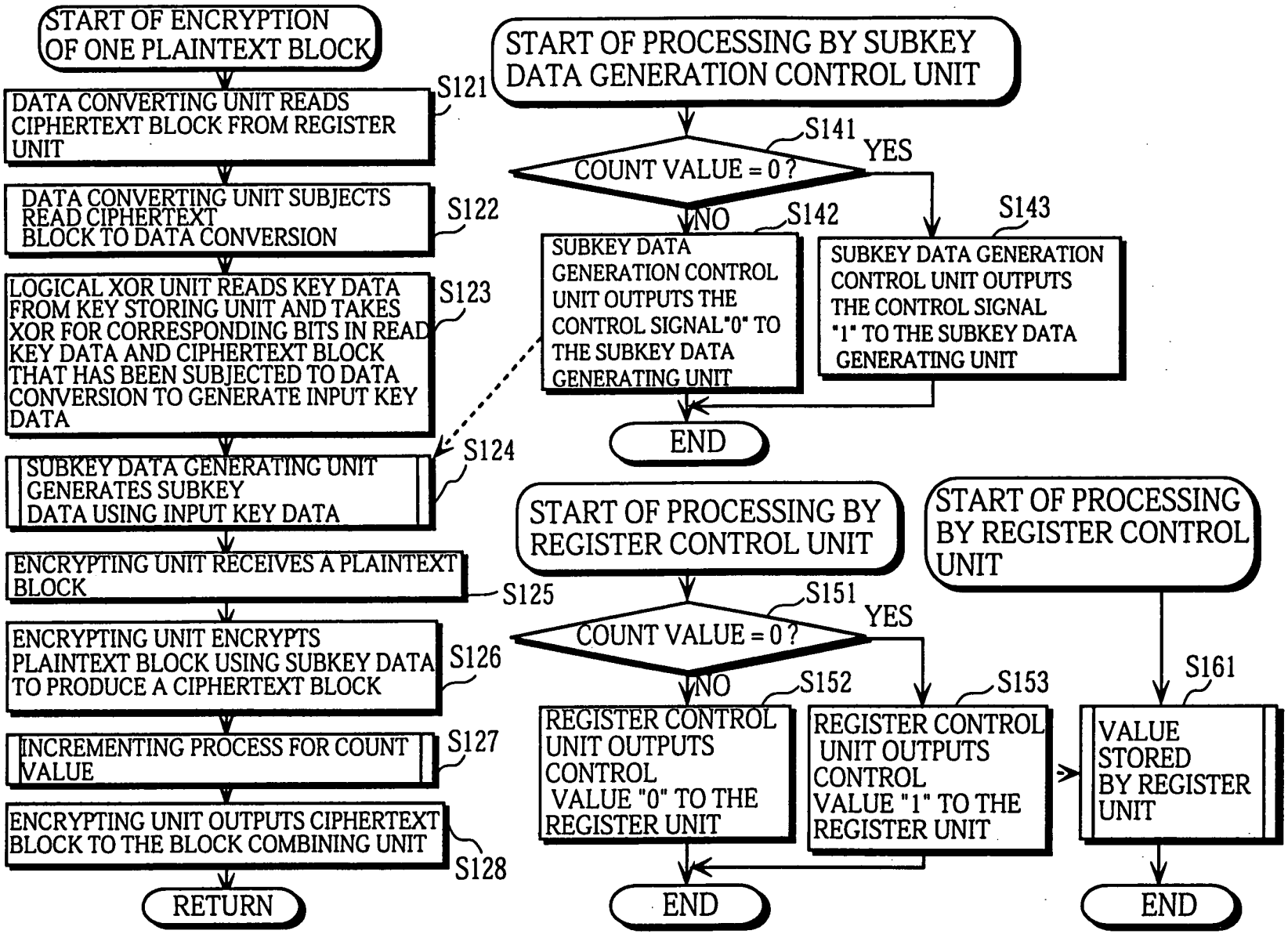
START OF ENCRYPTION OF ONE PLAINTEXT BLOCK
DATA CONVERTING UNIT READS CIPHERTEXT BLOCK FROM REGISTER UNIT
S121
DATA CONVERTING UNIT SUBJECTS READ CIPHERTEXT BLOCK TO DATA CONVERSION
S122
LOGICAL XOR UNIT READS KEY DATA FROM KEY STORING UNIT AND TAKES XOR FOR CORRESPONDING BITS IN READ KEY DATA AND CIPHERTEXT BLOCK THAT HAS BEEN SUBJECTED TO DATA CONVERSION TO GENERATE INPUT KEY DATA
S123
SUBKEY DATA GENERATING UNIT GENERATES SUBKEY DATA USING INPUT KEY DATA
S124
ENCRYPTING UNIT RECEIVES A PLAINTEXT BLOCK
S125
ENCRYPTING UNIT ENCRYPTS PLAINTEXT BLOCK USING SUBKEY DATA TO PRODUCE A CIPHERTEXT BLOCK
S126
INCREMENTING PROCESS FOR COUNT VALUE
S127
ENCRYPTING UNIT OUTPUTS CIPHERTEXT BLOCK TO THE BLOCK COMBINING UNIT
S128
RETURN
START OF PROCESSING BY SUBKEY DATA GENERATION CONTROL UNIT
S141
COUNT VALUE = 0 ?
YES
NO
S142
SUBKEY DATA GENERATION CONTROL UNIT OUTPUTS THE CONTROL SIGNAL "0" TO THE SUBKEY DATA GENERATING UNIT
S143
SUBKEY DATA GENERATION CONTROL UNIT OUTPUTS THE CONTROL SIGNAL "1" TO THE SUBKEY DATA GENERATING UNIT
END
START OF PROCESSING BY REGISTER CONTROL UNIT
S151
COUNT VALUE = 0 ?
YES
NO
S152
REGISTER CONTROL UNIT OUTPUTS CONTROL VALUE "0" TO THE REGISTER UNIT
S153
REGISTER CONTROL UNIT OUTPUTS CONTROL VALUE "1" TO THE REGISTER UNIT
END
START OF PROCESSING BY REGISTER CONTROL UNIT
S161
VALUE STORED BY REGISTER UNIT
END

FIG. 10

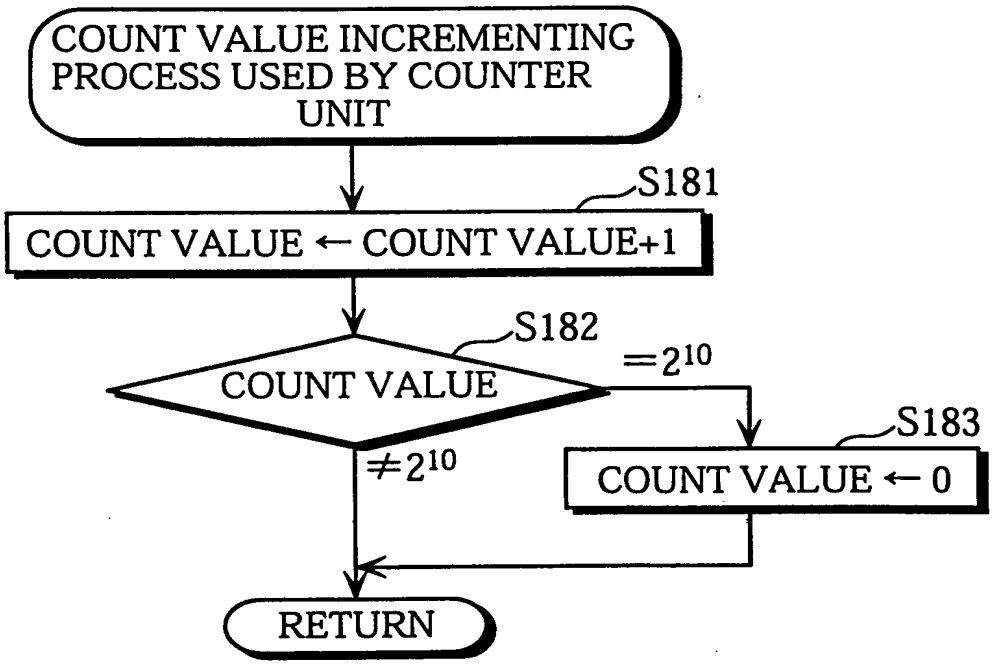
COUNT VALUE INCREMENTING PROCESS USED BY COUNTER UNIT
S181
COUNT VALUE ← COUNT VALUE+1
S182
COUNT VALUE
=2^10
≠2^10
S183
COUNT VALUE ← 0
RETURN

FIG. 11

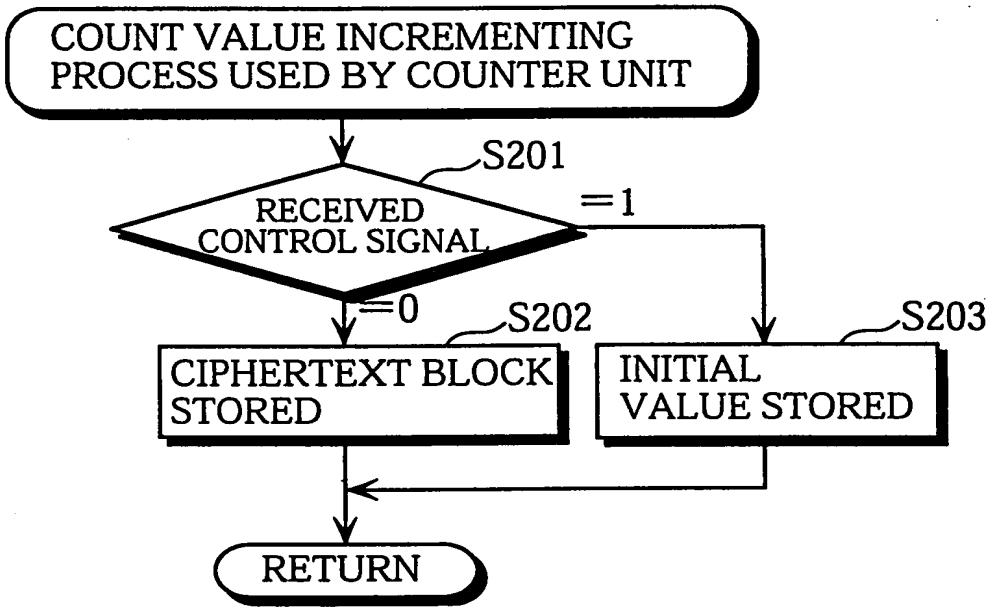
COUNT VALUE INCREMENTING PROCESS USED BY COUNTER UNIT
S201
RECEIVED CONTROL SIGNAL
=1
=0
S202
CIPHERTEXT BLOCK STORED
S203
INITIAL VALUE STORED
RETURN

FIG. 12

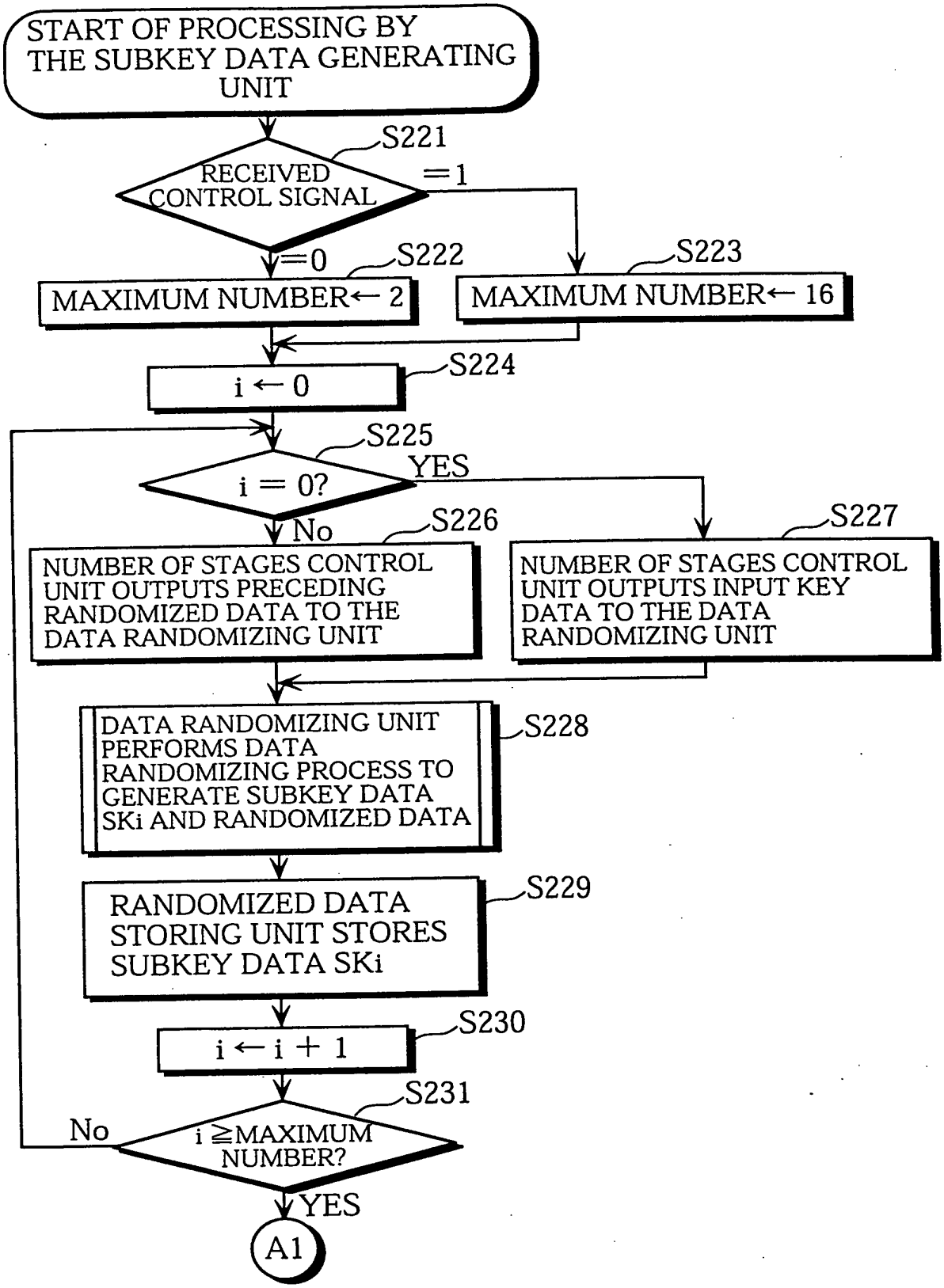
START OF PROCESSING BY THE SUBKEY DATA GENERATING UNIT
S221
RECEIVED CONTROL SIGNAL
=1
=0
S222
MAXIMUM NUMBER← 2
S223
MAXIMUM NUMBER← 16
i ← 0
S224
S225
i = 0?
YES
No
S226
NUMBER OF STAGES CONTROL UNIT OUTPUTS PRECEDING RANDOMIZED DATA TO THE DATA RANDOMIZING UNIT
S227
NUMBER OF STAGES CONTROL UNIT OUTPUTS INPUT KEY DATA TO THE DATA RANDOMIZING UNIT
DATA RANDOMIZING UNIT PERFORMS DATA RANDOMIZING PROCESS TO GENERATE SUBKEY DATA SKi AND RANDOMIZED DATA
S228
RANDOMIZED DATA STORING UNIT STORES SUBKEY DATA SKi
S229
i ← i + 1
S230
S231
No
i ≧MAXIMUM NUMBER?
YES
A1

FIG. 13

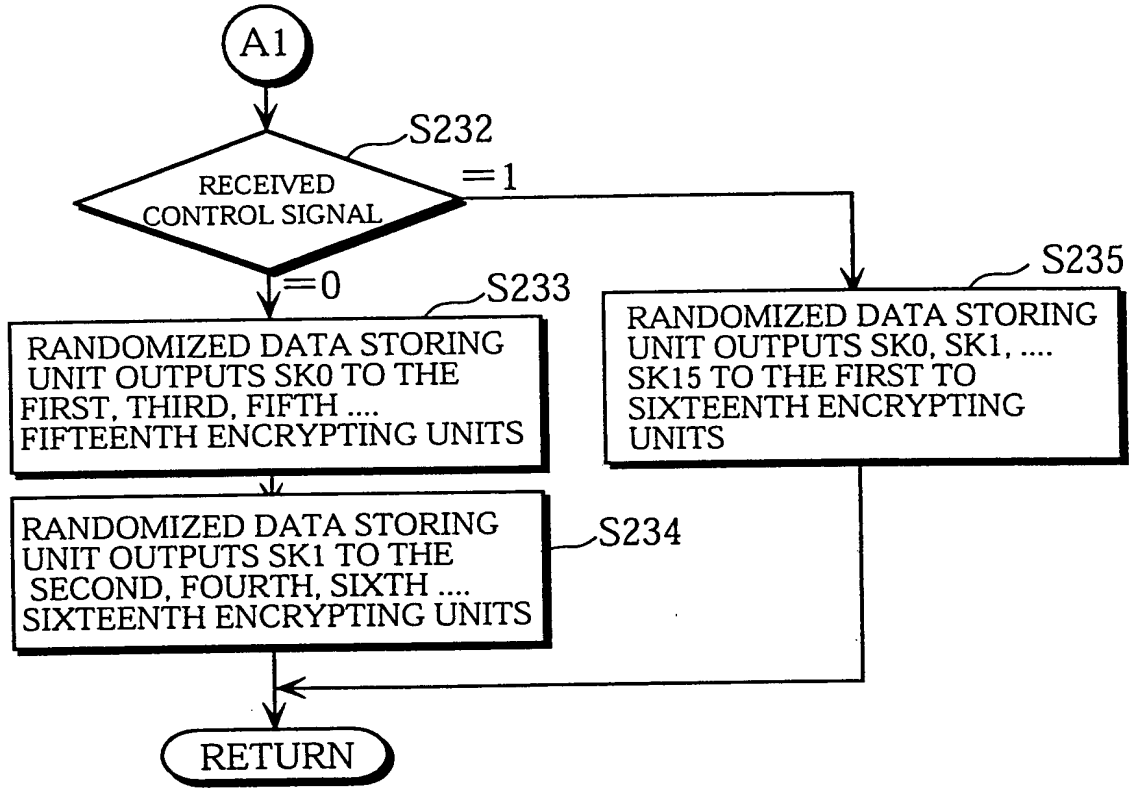
A1
S232
RECEIVED CONTROL SIGNAL
=1
=0
S233
RANDOMIZED DATA STORING UNIT OUTPUTS SK0 TO THE FIRST, THIRD, FIFTH .... FIFTEENTH ENCRYPTING UNITS
S235
RANDOMIZED DATA STORING UNIT OUTPUTS SK0, SK1, ... SK15 TO THE FIRST TO SIXTEENTH ENCRYPTING UNITS
RANDOMIZED DATA STORING UNIT OUTPUTS SK1 TO THE SECOND, FOURTH, SIXTH .... SIXTEENTH ENCRYPTING UNITS
S234
RETURN

FIG.14